Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:25:29 UTC

Tool: Kerberods

Names	Kerberods
Category	Malware
Type	Dropper, Worm
Description	(Trend Micro) Kerberods is responsible for dropping the cryptocurrency miner (khugepageds, detected as Coinminer.Linux.MALXMR.UWEJI) and its rootkit component. One particularly interesting aspect of the binary is the way it drops the rootkit. Kerberods also has multiple ways of propagating itself, spreading via SSH and exploiting CVE-2019-1003001 and CVE-2019-1003000.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.kerberods>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:kerberods>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Kerberods

Changed	Name	Country	Observed	
Other groups				
	Rocke, Iron Group		2018-Apr 2021	

1 group listed (0 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b2f59574-e769-4655-8b30-28e7c608bf41